Understanding users' health information privacy concerns for health wearables

Moritz Becker
LMU Munich
m.becker@bwl.lmu.de

Abstract

Health information privacy concerns (HIPC) are commonly cited as primary barrier to the ongoing growth of health wearables (HW) for private users. However, little is known about the driving factors of HIPC and the nature of users' privacy perception. Seven semi-structured focus groups with current users of HWs were conducted to empirically explore factors driving users' HIPC. Based on an iterative thematic analysis approach, where the interview codes were systematically matched with literature, I develop a thematic map that visualizes the privacy perception of HW users. In particular this map uncovers three central factors (Dilemma of Forced Acceptance, State-Trait Data Sensitivity and Transparency) on HIPC, which HW users have to deal with.

1. Introduction

Health information privacy concerns (HIPC) constitute a barrier to the ongoing growth of health information technologies comprising digital medicine, electronic medical records or remote patient monitoring [1]. Owing to the high sensitivity of the gathered personal health information (PHI), privacy concerns have proved to be more important in the context of such health technologies than other technological devices [2]. However, to date, no study has offered a comprehensive conceptualization of users' privacy perception and there is no empirical evidence of the main factors influencing users' HIPC. The "understanding of information privacy remains fragmented in the under examined health context" [3] and in particular for wearable health technologies [4].

Arising from the intersection of healthcare, health informatics, and information systems, health wearables (HW) for private users continuously monitoring a range of PHI from illness to fitness without the need of health professionals (e.g. physicians) [5]. Therefore the HW user becomes a real-time "walking data generator" [6, p. 63], and HIPC occur by exposing such PHI without awareness or consent [7]. "In order to address and appease individuals' HIPC, it is imperative to identify and understand how different factors influence individuals' HIPC" [3, p. 9]. As privacy concerns are complex psychological concepts in the individual minds [e.g. 8], I use a thematic analysis approach to structure the heterogeneous privacy perceptions into homogeneous themes to compare and analyze the influencing factors on HIPC of HW users. Uncovering the nature of users' privacy perception and identifying the driving factors of HIPC could "help researchers and designers understand the major dimensions that are critical in their work" [9, p. 497]. I ask: *What factors influence the HIPC of HW users?*

To answer this research question, I use the HIPC Model by Kenny and Connolly [3] to explicitly address privacy concerns with health information technologies. I conduct seven semi-structured focus groups with six users of HWs each and apply a rigorous iterative thematic analysis to empirically understand users' mindsets regarding their HIPC. This "method for identifying, analyzing, and reporting patterns within data" [10, p. 6] has been successfully employed to uncover user perception of health apps, or compare privacy concerns of digital services [11]. By reviewing the conducted codes on literature, I enhance the theoretical understanding of HIPC by proposing three central factors (Dilemma of Forced Acceptance, State-Trait Data Sensitivity and Transparency). This thematic map enables researchers to uncover the understanding of privacy perception of HW users and help practitioners to develop privacy-friendly devices.

2. Theoretical background

2.1. Health information privacy concerns

Previous studies primarily use the privacy calculus theory to analyze individuals' willingness to share PHI voluntarily if they expect that perceived benefits from data disclosure outweigh the perceived

URI: http://hdl.handle.net/10125/50301
ISBN: 978-0-9981331-1-9

costs [e.g. 12, 13]. This tradeoff theory has been described as "the most useful framework for analyzing contemporary consumer privacy concerns" [14, p. 326], but still underscores the risk-control interplay. Both risk and control have been shown to operate as privacy-borne beliefs relating to the potential consequences of PHI disclosure [15]. For health technologies, improper information practices would result in the mining and mapping of personal data to make an individual's health status more visible. The collected PHI may be easily analyzed, distributed, and re-used, and users perceive a relatively high risk that the provided PHI is being put into secondary use for unrelated purposes without their knowledge or consent [13]. Thus, the sensitivity of various datasets such as demographics, activities (e.g. accelerometers, pedometers, location), or physiologies (e.g. electrocardiograms, pulse oximeters, blood glucose meters, and weight scales) in particular, have prompted heated discussions about individuals' health information privacy [4, 16]. Health information privacy "is an individual's right to control the acquisition, uses, or disclosures of his or her identifiable health data" [17, p. 1]. Kenny and Connolly [3] developed the Health Information Privacy Concerns Model (HIPC) to explicitly address privacy concerns with health information technologies. The HIPC is composed of the six constructs Collection, Unauthorized Secondary Use, Improper Access, Errors, Control and Awareness [18]. The first four dimensions are affiliated to the Concerns for Information Privacy-Model (CFIP) [19]. The two remaining dimensions, *Control* and *Awareness*, derive from the Internet Users Information Privacy Concerns-Model (IUIPC) [20].

The construct *Improper Access* is considered especially important concerning high sensitive data environments [11]. It describes privacy concerns with respect to the perceived threat of unauthorized access by third parties. Several earlier studies have shown that potential access of third parties (e.g. employers or insurances) to private health data is a common cause of concern for individuals [15].

Data inaccuracies have been a major issue in studies on health technologies [4]. The construct *Error* considers users' concerns for data inaccuracies. Individuals believe the digitization of health data can generate more errors [11]. It can be assumed that third parties such as insurance companies will only contribute to the integration of technologies in a healthcare system, if companies provide accurate data. Therefore, user insights on measurement accuracy are considered crucial [3].

The dimension *Unauthorized Secondary Use* addresses users' concerns that their data is utilized for other than the agreed upon purposes, such as marketing purposes. If individuals believe these potential uses may occur, they are likely to express HIPC [18].

Studies show that individuals are concerned regarding the electronic collection and storage of their PHI [e.g. 1]. The dimension *Collection* describes this subjective concern with respect to the accumulation of PHI [3].

Hong and Thong [18] showed that perceived control over the disclosed PHI is an important influencing factor for users during their interaction with websites. The Control dimension covers the individual's concerns that they do not have adequate control over their PHI [20].

The sixth dimension *Awareness* refers to the individual's concern regarding their lack of awareness of how a device uses and protects the privacy of their PHI [20]. Studies assume that users are to a large extent unaware of the potential for data misuse through the digitalization in health [21]. Kenny and Connolly hypothesized that an increased awareness leads to higher privacy concerns. However, they found support for this hypothesis in only one of their two samples [3].

2.2. Health information privacy concerns of health wearables

To empirically explore the influencing factors that drive these six dimensions of HIPC I use HWs as one of the most distributed health technology for private users [4]. I define HWs as small digital devices with biometrical sensors designed for private users and worn on the body to continuously generate PHI without the need for health professionals. By continuously collecting PHI and analyzing these data in real time HWs provide instantaneous, goal-oriented feedback. Therefore individuals have the chance to understand their health status to reveal possibilities for improvement. The collected PHI can be stored stationary on the mobile device, the computer or digitally in a cloud [13].

Owing to the high data sensitivity and the mobility of the devices, privacy concerns have proved to be more important in the context of HWs than other technological devices [e.g. 2, 22]. In contrast to medical health wearables for professional usage or other clinical devices, in which electronic health records are created and managed by healthcare providers (hospitals and other clinical organizations), HW users create and manage their PHI without the help of physicians [23]. While physicians are usually required to keep users data confidential, this will be subject to further legislator assessment in the case of

HWs. As HW analysis outcomes are immediately available in digital form, their dissemination to third parties is easy and can be lucrative for suppliers, but it can also harm users' privacy. Many HWs collect and store PHI in online portals to connect users to their health status and provide goal-oriented feedback as needed [4]. Therefore, the technology not only improves users' knowledge about themselves, but especially the providers' knowledge about the users [e.g. 8, 9]. Providers even share data with third parties, as for example with healthcare providers and insurance companies to adjust insurance premiums according to the analyzed data sets, which can lead to a worse economical outcome [1].

3. Methodology

3.1. Thematic analysis of focus groups

I chose a qualitative approach to examine the factors that influence the HIPC (Collection, Unauthorized Secondary Use, Improper Access, Errors, Control and Awareness) of HW users. As focus groups are especially well suited to uncovering and documenting the 'why' behind opinions, and in obtaining much more depth and breadth of analysis from participants than available from individual data collection methods [24], I conducted semi-structured focus groups with current users of HWs. As focus groups allow participants to query each other, explain themselves and comment on each other's experiences [25], this research method is frequently used to evaluate critical healthcare themes [25] and has been already used to uncover privacy aspects [e.g. 11]. The interview guide for the group sessions were developed on the six dimensions of the HIPC model. The interview evaluation is based on the thematic analysis approach, as it is a well-established method of qualitative data analysis [10]. Thematic analysis is a method for identifying, analyzing, and visualizing patterns within data and is especially appropriate for analysis in sensitive data environments [e.g. 26]. It has been successfully employed to uncover user perceptions of health apps or critical experiences with self-tracking in information systems research [27]. By organizing and describing the data set in rich detail, it normally goes even further by interpreting various aspects of the research topic [26].

3.2. Data collection

Considered to be an adequate number [24], seven focus groups were conducted to capture the privacy perception of 42 current HW users. To ensure participants represented a broad range of experiences and ages, I used peer recruitment for all of the seven focus groups (opportunistic sampling). The groups were designed to encourage participants to interact with each other, rather than the researcher, allowing "structured eavesdropping" [25, p. 301]. At the start of each session the researcher provided an overview of the objectives of the study. Afterwards, the researcher attempted to restrict their own contribution to reading the six questions concerning the six dimensions of the HIPC model out aloud, and only asking further probing questions when required. Each focus group lasted approximately one hour, with 10 min spent discussing each question. The use of the same questions and procedure for each focus group facilitated investigation into the similarity of the themes discussed across the focus groups [11].

Table 1. Demographic profile of participants

Demographics		Number of respondents
Gender	Male	20
	Female	22
Age	Average	37
Education Level	None	3
	High/Secondary School	7
	Bachelor	6
	Master	14
	PhD	10
		2
Employment Status	Employed	22
	Self-employed	10
	Student	9
	Unemployed	1

3.3. Data analysis

I follow a rigorous iterative thematic analysis approach that matches the interview codes, factors and dimensions by constantly reviewing literature. Figure 1 provides a detailed illustration of the methodological approach, which was not a linear phase-to-phase process, but a recursive one, by moving back and forth between the different phases of the analysis. First, I transcribed the focus groups' audio recordings and then repeatedly read through the transcript. Afterwards I generated initial codes by searching for recurring patterns in the raw data. In this way, I could aggregate the data to workable items. I identified 39 different codes in the data set. In the next step I merged different codes with factors – e.g. users who based their willingness to disclose information on the identity of the data recipient or the perceived sensitivity of their data. Consequently, the two respective codes Recipient-specific Data

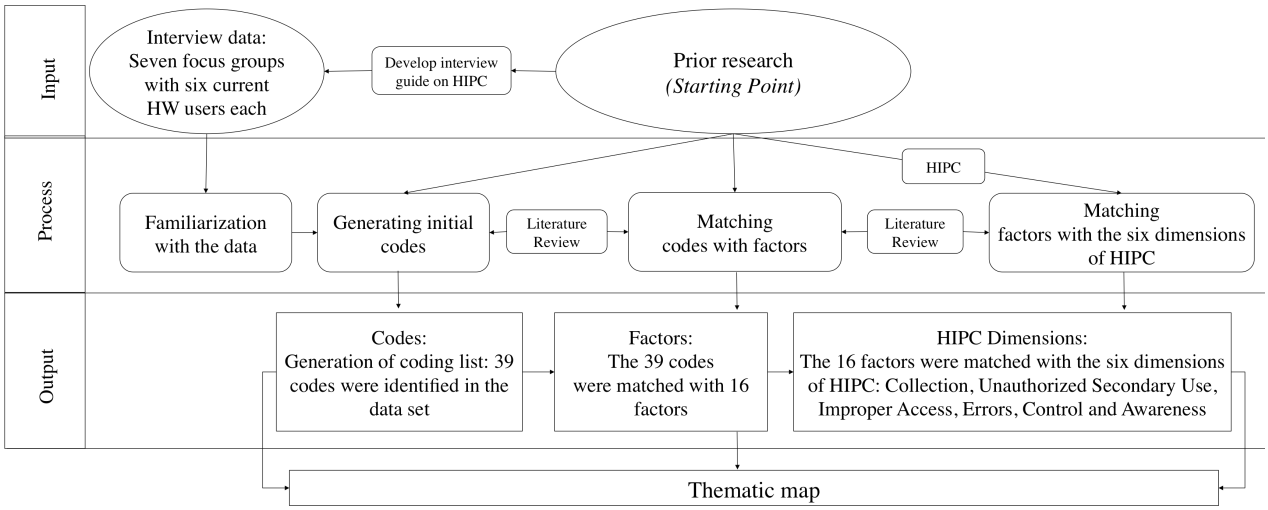

Figure 1. Iterative thematic analysis approach

Retention and Sensitivity-specific Data Retention were matched to the factor Contextualization. The process of matching codes with the factors, and then the factors with the six dimensions of HIPC was accompanied by a constant review of the literature.

4. Results

The thematic map visualizes the results. It is composed of the six dimensions of HIPC Collection, Unauthorized Secondary Use, Improper Access, Errors, Control, Awareness [3] and their related 16 factors (Figure 2).

4.1. Collection

The Collection dimension captures an individual's concerns that a device is collecting and storing large quantities of their PHI [3, 19]. Three factors were related to this dimension.

Deanonymization: Users are not aware of the degree of anonymization of their PHI. Although users wish for an anonymized storage of data, they do not eliminate the possibility of personalized storage: *"I hope my fitness activities are anonymized, it would be terrible if my fitness trainer could see them!"* [P8] Some users were afraid of a Deanonymization through the connection of primary and secondary data: *"There just needs to be a combination of two databases and anonymization is worthless."* [P28]

Location of Data Storage: Users are concerned about the location of data storage and analysis: *"Although I am wearing the device on my body and data are shown on the display, I am pretty sure that they are saved in a cloud."* [P23]

Data as Asset: This factor reflects that many users perceived PHI disclosure as beneficial. One respondent who used his fitness tracker to fight obesity perceived his PHI as a means to externally verify his healthy lifestyle. He described the reaction of his physician when he first showed him his fitness trackers, as follows: *"When I visited my doctor and was asked for my current blood pressure, I could show the measured value on my health wearable. The doctor really appreciated that."* [P7] A lot of users valued the collection of PHI to monitor their fitness activities.

4.2. Unauthorized secondary use

The Unauthorized Secondary Use dimension relates to an individual's fear that their PHI is collected for one purpose but used for additional purposes without obtaining their permission [3, 19].

Cross-connection: The first factor concerning Unauthorized Secondary Use describes the unconscious worries over the connection of data with other databases. The users have little or no knowledge regarding whether this connection happens in reality: *"I do not know whether apps and devices are communicating and exchanging data."* [P3] Some users assume that, by using the device, there is an automatic authorization for the business partner to use, analyze and pass on the data: *"Of course, they will save all of my available data and create a profile to optimize the evaluation."* [P17] Additionally, users think cross-connection carries a high possibility for errors: *"My device is not able to count my steps appropriately, how should it be possible to connect and analyze different data sources and create predictions?"* [P36]

Trust Cues: The study participants are aware of the possibility that data could be sold to third parties. During the conversations, the usage of the word *"hopefully"* is striking when talking about the anonymization of data. This shows the concerns about personalized data transfer. Furthermore, the nescience about laws and rights concerning the usage and transfer of data causes further concerns, especially regarding the degree of anonymization: *"They got the data and if it is legal, they will use them. But hopefully, the data are anonymized."* [P12]

Contextualization: This factor refers to the observation that users compared their disclosure of PHI to their disclosure behavior in other contexts and decided to reveal personal information based on the perceived comparative sensitivity of the PHI. So, one user states that she foregoes privacy consciously, because otherwise she could not use a new feature. Other participants with similar views state that there is a trade-off between costs and benefits depending on the context. P30 states: *"Sometimes I do not think about my privacy, it is more important to me to use the device quickly and that everything is running."* Almost all focus groups were open-minded towards a transfer of anonymized data for medical research purposes. Users were reluctant to make their PHI accessible to third parties, but were open-minded to its use by employees to improve the tracker: *"I do not care about usage of data by software developers who want to improve the trackers. I would even support it!"* [P15] Other users were indifferent towards disclosing their PHI to friends, but reluctant to make it accessible to providers: *"I like to share my eating habits with friends but I am concerned about sharing it with my insurance company."* [P1]

4.3. Improper access

The Improper Access dimension covers individuals' concerns that devices do not have adequate measures in place to prevent unauthorized individuals or organizations from accessing their PHI [3, 19]. Users of HW are aware of security gaps but differentiate depending on access route between a passive improper access (Provider Complacency) and an active improper access (Hacking Hazard).

Provider Complacency: Describes the unauthorized access by third parties which happens incidentally or passively because of insufficient privacy adjustment options. *"For instance, Fitbit's default privacy settings inadvertently exposed information about some of their users' sexual activities."* [P21] Users are especially concerned about the privacy complacency of companies financed by venture capitals, as the goal of fast economical success is often more important than the implementation of privacy features or the identification and closing of security gaps. So, neither *"the brand nor the reputation"* [P35] can be affected and *"companies try to be the first one in the market, so privacy will not be placed first."* [P33] P36 adds: *"Providers cannot make any money with privacy – that is theme is just expensive for these firms."*

Hacking Hazard: This factor summarizes the observation that users are afraid of being hacked if they are part of a bigger data collection. The more data a company collects, the higher the objection and *"then it is just a matter of time until you get attacked."* [P25] However, users had no concrete idea of the extent and the consequences of this active improper access.

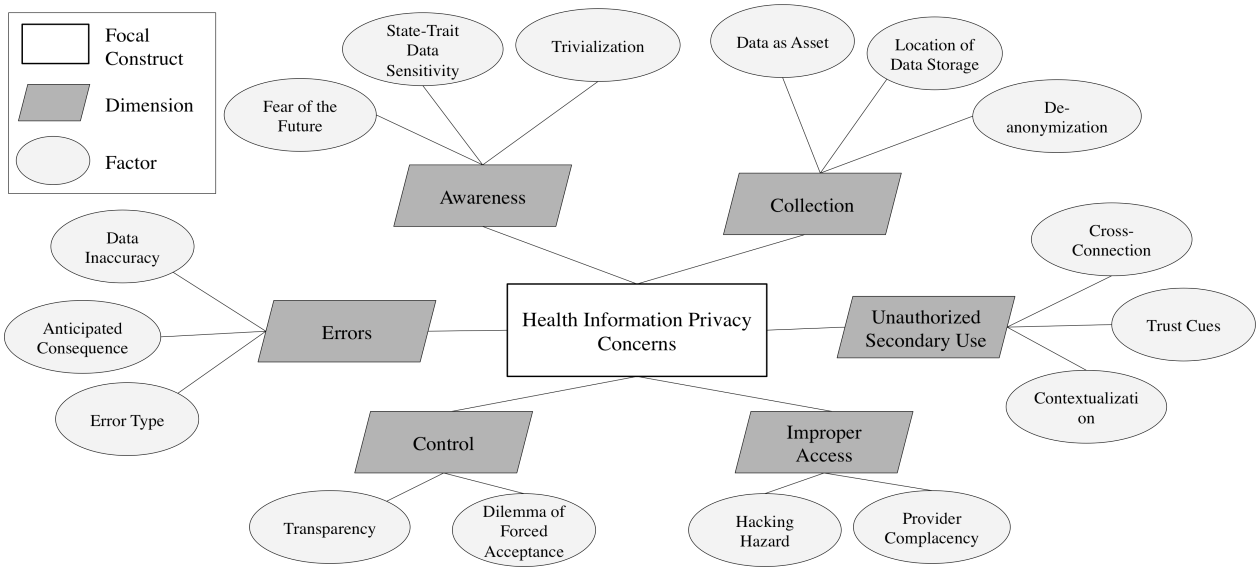

Figure 2. Thematic map of privacy perceptions of health wearable users

4.4. Errors

The Errors dimension relates to the individual's concerns that devices do not have adequate measures in place to prevent or correct errors in their PHI [3, 19].

Data Inaccuracy: This factor describes the extent to which users experienced inaccurate data measurements or functional disorders of HWs. When it comes to the accuracy of the produced data, users state that the recorded data are mostly just *"semi-precise"* [P2] or *"also inaccurate"* [P7] and a general *"deviation of up to 15% is acceptable."* [P16] Based on their own experiences, some users described aspects, which influence data accuracy negatively. In general, users are not concerned about privacy aspects, if there is less data inaccuracy.

Anticipated Consequence: The users separate the consequences of incurrence data between two usage scenarios of HWs. In the first usage scenario (private focus), users accept approximate values for the rough estimation of the performance as long as the generated data serve no medical purpose or will be passed on to health insurances. P5 states: *"Whether the indicated 8,567 steps on my tracker were recorded correctly, does not matter for me as long as my health insurance or other institution do not get the PHI."* In the second usage scenario (professional health focus) users are afraid that approximate values of the generated PHI could lead to erroneous allocations within tariff systems, or could be used for medical diagnoses or treatments. So, some focus groups discussed the opportunity to falsify the data actively and consciously. *"I think the topic is very sensitive, because we do not know who controls it."* [P3] P1 comments on that: *"I buckle the device to my dog and get it to chase a ball in the garden."*

Error Type: Four of the seven focus groups discussed different error types and their effects. Type one errors represent the occasions when flawed data leads to misleading feedback, which incorrectly diagnoses lack of activity or other issues, or even diseases. Users relying on this information, instead of a professional medical evaluation, can misdiagnose themselves, resulting in dangerous self-treatment. Type two errors relate to the possibility that devices can miss symptoms which indicate the presence of an issue or disease, resulting in the owner being described incorrectly as healthy and active. P29 summarizes: *"Without a doctor's advice, users do not choose an appropriate level of activity to get well again, resulting in harm through overextending themselves with too much physical activity. And this could be very dangerous.*"

4.5. Control

The Control dimension covers an individual's concerns that they do not have adequate control over their PHI [3, 20].

Transparency: On the one hand, users were aware of the collection and storage of their PHI for individualized evaluations (e.g. progressing statistics). On the other hand, a lot of users possessed neither an overview of the extent of data collection, nor the control between primary and secondary data analysis. *"I am aware of the storage of my data as they are needed for personal feedback but I have no idea about the further use of my health data."* [P23] In particular, users have little or no insight into which data are analyzed, in which way, and how to control this: *"I can control when to wear or not to wear the device, but there is no transparency of data control."* [P21] P22 adds that: *"I think there is always a disparity between the amount of data recorded and the data shown to the user."*

Dilemma of Forced Acceptance: P6 describes the dilemma of the HW users: *"I am either forced to use the device and know about the data recording and the possible usage of the data or I decide against the usage consciously."* From the users' perspective, a comprehensive control of the PHI recorded by the HW is no longer possible. They see the conscious renunciation of such devices as the only way out. Thereby, the consequences of a conscious renunciation of HWs are seen as *"a step back to a bygone age,"* [P2] where the *"numerous advantages of the technological development did not exist."* [P27] Many users highly doubt whether such a release is possible at all: *"I would like to have more control about my data, but you have to accept how it goes. Beggars cannot be choosers."* [P7] All focus groups discussed this compulsive acceptance of HWs. Post-purchase lock-in effects were of particular concern: *"Once I have bought the product and then, for example, terms and conditions change afterwards, I would probably accept all privacy restrictions and continue to use the product because of the money invested and the activity records that had already been tracked."* [P25]

4.6. Awareness

The Awareness dimension refers to the individual's concern regarding their lack of awareness of how a device uses and protects the privacy of their PHI [3, 20].

State-Trait Data Sensitivity: The participants perceive the data generated by the HW as sensitive and private. *"These are data from my internal body,*

it couldn't be any more sensitive!" [P12]. Nevertheless, users perceive data sensitivity differently, with a differentiation between personal and device data sensitivity: The device data sensitivity summarizes the observation that users differentiate depending on the device focus. Devices with a health and medical focus are associated with higher data sensitivity and devices with a fitness and lifestyle focus are related to lower data sensitivity. Independent of the device, the users described different personal data sensitivities. Some users described the data tracked by a device as *"extreme"* [P6], *"high"* [P12] or *"ultimate"* [P16] sensitive, whereas other users perceived them as *"not as sensitive as bank- or identity documents."* [P22] P29 summarizes: *"I think most of the users are aware of the data sensitivity. But as with many things in life, for one user they are more sensitive than for the other."*

Trivialization: Within the user groups, the participants often make statements like: *"It is not that bad, the government will monitor this and will intervene if necessary."* [P22] *"I have nothing to hide, they can access my data."* [P2] More than the half of the users expressed such statements. These verbalized trivializations show a helplessness of the users. *"I think we trivialize the whole situation because we are able to change something, if we want to use the devices entirely."* [P34]

Fear of the Future: This factor summarizes the observation that many users are worried about the future: Some users ask themselves where the technical developments are leading to, and where the limits will be set with regard to privacy. *"The next generations know only complete digitalization, so the sensitivity will decrease and the indifference will increase. I am honestly worried about where this is leading to."* [P33]

5. Discussion

This study was motivated by the research call to "identify and understand how different factors influence individuals' HIPC" [3]. To understand the factors that drive HIPC I used HWs as one of the most distributed health technology for private users [4]. Seven semi-structured focus groups with a rigorous iterative thematic analysis were evaluated to empirically understand the HIPC of HW users. Based on this iterative approach that constantly matches the interview codes, factors and dimensions on literature, I used a thematic map to visualize, share and discuss the findings deriving from the qualitative data analysis. This thematic map visualizes the structure that best represents users' perceptions of HIPC distinguishing on the six dimensions of HIPC (Collection, Unauthorized Secondary Use, Improper Access, Errors, Control and Awareness) and their 16 factors. While the different focus groups and their participants have proposed a large number and variety of different points of interest, three factors (Dilemma of Forced Acceptance, State-Trait Data Sensitivity and Transparency) stood out in terms of frequency of mentioning as well as discussion length and intensity. These three factors were discussed in all focus groups and were mentioned by more than 90 percent of the users.

Dilemma of Forced Acceptance: Despite the fact that many users perceived the PHI collection of their devices as a threat to their privacy, some users also voiced sympathy for PHI disclosure. This contrasts the mainstream privacy research on wearable health technologies, where privacy is often exclusively treated as a user-side threat [2]. In my study, PHI disclosure was valued as an ability to monitor personal activities or as a source of potential monetary compensation by insurance companies. Although this implies people consider the risks and benefits of providing PHI to some degree, the factor Data as Asset relating to the benefits offered by HWs, indicates users are principally focused on the benefits they believe they will receive for disclosing PHI. So almost all users report a Dilemma of Forced Acceptance of HWs where HIPC are mainly caused by lack of control, but the advantages of HWs are so predominant, that a conscious renunciation is not possible. Many users have already given up trying to do something about high HIPC and now accept the situation, as they do not see any possibility for action with regard to this dilemma. These users "seem to be likely to accept constant monitoring [of PHI] through sensors because they are persuaded that the benefits outweigh the costs" [28, p. 11]. Consequently, the majority of the participants could be described as users of HWs that see themselves, as "beggars that cannot be choosers." These users process the Dilemma of Forced Acceptance with the two factors of Awareness (Trivialization and Fear of the Future). On the one hand users handle the situation by understating their HIPC and hope for legal support (Trivialization). On the other hand users deal with this dilemma by pushing it further into the future and formulate dark future prospects, so they do not have to deal with it now (Fear of the Future). State-Trait Data Sensitivity: The factor State-Trait Data Sensitivity confirms other research studies [e.g. 3, 15] which show that the more sensitive individuals perceive PHI to be, the greater their concerns are regarding the privacy of this data. My qualitative results are in accordance with Li, Wu, Gao and Shi

[13, p. 15], who noted that "health information sensitivity (has) significant effects on individuals' perceived privacy risk." But my results indicate this factor should be divided into two components of State-Trait Data Sensitivity. First, a personal component (personal data sensitivity) referring to the observation, that data sensitivity varies from one individual to another. In this sense personal data sensitivity could be seen as a trait factor [15], where an individual that has higher personal data sensitivity will likely be more concerned over its use, storage, and privacy, than a person with a lower personal data sensitivity. The second component (device data sensitivity) refers to the observation that users perceive that fitness and lifestyle-focused devices collected less sensitive PHI than health- and medical-focused devices. This result confirms previous studies in which researchers reported that individuals found health or medical data much more sensitive than other information such as demographic, lifestyle habits, or purchasing behaviors [1]. Kenny and Connolly [3] called this "from illness to fitness", while Alrige and Chatterjee [9] differentiated between monitoring (medical), prevention (fitness), and communication (lifestyle) situation and devices. This State-Trait Data Sensitivity is also reflected in the factors Anticipated Consequences and Contextualization. First, the users separate the consequences of inaccurate data between two usage scenarios of HWs. Therefore, users accept approximate values for the rough estimation of the performance as long as the generated PHI serve no medical purpose. If the device has a professional health focus the users are afraid that approximate values of the generated PHI could lead to incorrect allocations within tariff systems or could be used for inaccurate medical diagnoses or treatments. Second, HIPC for HW users were context-related (Contextualization). Users of HW compared their attitude towards the disclosure of PHI to their disclosure behavior in other contexts [12]. Many users decided to reveal personal information based on the comparative sensitivity of the health-related information. That means they would not shudder to publish PHI for when they perceived the disclosed PHI as equally or less sensitive to the personal information they provided to other companies in other contexts. Furthermore, users of HW were far more positive towards PHI disclosure for the purpose of medical research purposes or product improvement, than for transferring PHI to third parties.

Transparency: Initiated by the technical possibilities through Cross-connection, Deanonymization and Location of Data Storage, almost every participant reported a perceived loss of transparency when using HWs. This factor, was also stated to be a strong trigger for HIPC in other studies of health technologies [e.g. 11, 29]. Not only does this lend credence to the idea that people principally seek informational self-determination when engaging with technology services, but also echoes one of the factors—control over collection and usage PHI—in the IUIPC scale [20]. Validating the CFIP scale, Stewart and Segars stated that, "a central concern that seems to underlie consumer attitudes, and is perhaps the common theme captured by the higher-order concept of CFIP, is the issue of control. Consumers desire levels of personalization and customization but also want some sense of control over how this service occurs" [30, p. 46]. This control-based privacy dilemma is already discussed in privacy literature [e.g. 11], and confirmed in other empirical studies [e.g. 20]. Although Control was identified as an important dimension of HIPC [3], for HW users the PHI control is more than the disclosure or non-disclosure of information. It is a decision making process in which the HW user considers the HW usage scenario (private focus vs. professional health focus), of engaging in a particular behavior. As new technologies affect this calculus of behavior [11], individuals are often unable to predict the nature of that which has to be managed. This understanding of a behavior calculus underpins Culnan and Bies' observation that a "social exchange perspective also applies to a consumer context" [14, p. 327] or, in my sense, a consumer health context.

6. Implications and Conclusion

6.1. Implications

This study has important theoretical and practical implications. The thematic map provides researchers with a visualized structure of what determines a user's HIPC and can be seen as a strong initial insight into the main drivers of HIPC. It is acknowledged that other factors may be influential, but it is maintained that this thematic map represents a strong starting point. Therefore, results from this study can contribute to the understanding of HIPC and identify possible avenues for future research. For instance further research could prove the relationship between the developed factors and the dimensions of the thematic map in a quantitative study.

Moreover, the findings of this study could support theory-building efforts to uncover the meaningful interplay between HIPC and perceived benefits in the user's mind. This multifaceted picture of a user's

mental trade-off decision, in particular concerning the Dilemma of Forced Acceptance and the Transparency opens new research directions. Therefore, the developed factors will further enhance the understanding of the role information privacy plays in health context and will strengthen the literature by extending constructs concerning HIPC and PHI disclosure [13].

The thematic map can serve as a practical guideline for providers to develop privacy-friendly devices. The study results can serve as an important building block in privacy requirements engineering for healthcare information technologies [21] and corresponding privacy-enhancing technologies [7]. This is especially relevant as the General Data Protection Regulation (GPDR) coming applicable in 2018. Providers must strategize privacy alignment for their products by incorporating in their design the privacy and data protection capabilities necessary for regulatory compliance and gaining user trust.

First, users did not want their PHI to be used for purposes other than the ones agreed upon between them and the provider. The provider could decrease HIPC, by increasing their transparency about data storing and dissemination. Individuals made their data retention dependent on both the usage scenario and the severity of PHI [12].

Second, the results show that the Control is an important dimension in user mindsets concerning HIPC. Furthermore, some of study participants wanted providers to protect their PHI irrespective of costs. This signals that providers need to gain trustworthiness by addressing those privacy concerns through a transparent information policy [16]. Consequently, to increase customer satisfaction and market reach, providers need to reveal the identity of third parties accessing the data, the purpose of the data usage and the objectives for which the data is used. So a company, which focuses on the perceived lack of control and gives the user a feeling of control over the data, could reach a unique selling point over the competitors. This unique selling point could then be a reason to buy the device from this specific company.

Third, despite these insights into decreasing the HIPC by increasing the control of PHI, providers could utilize the users Dilemmas of Forced Acceptance. As most of the users see themselves as "beggars are not choosers", and want to use the devices independently of their HIPC, companies should minimize the barriers to entry for the first usage of the device and clearly communicate the benefits. So companies could win new users, e.g. through low prices and free extra features independently of HIPC with the intent that "once a user, always a user".

6.2. Limitations and further research

An obvious limitation of this study was the small sample size of 42 people who took part in the focus groups. However, as this was an exploratory study involving focus groups, and the "[…] common rule of thumb is that most projects consist of four to seven focus groups" [24, p. 144], an average of six participants in each focus group is reasonable.

A major advantage of focus groups—their ability to encourage group level discussion—is potentially one of their major limitations. Participants may behave differently if faced with the device assigned to their focus group in a different context (e.g. using it alone to achieve a specific goal). To avoid this, peoples' stated privacy behavior is sometimes not the same as their actual behavior.

In focus groups, people may be more truthful about their privacy behavior in front of others who may challenge them and ask for justification of their views. In focus group discussions, people may be reminded by other participants of factors they would not normally consider, and therefore there is a danger of dominant personalities steering a group's discussion. Both biases were mitigated to some extent by the study's design. Firstly, the use of a standard set of six questions, with an approximately similar amount of time allotted to each question, ensured discussion remained focused. Secondly, the researcher ensured that the discussion was not hijacked by particular participants.

The definition of HWs excludes medical devices, in which health professionals diagnose and evaluate users' medical problems. Therefore, it would be interesting to compare the study results and especially the developed thematic map with patients suffering chronic diseases or in general with users of professional medical devices and analyze whether additional dimensions or factors of HIPC emerge.

The focus groups consist of actual users of HWs, not potential ones. For these the benefits of HWs obviously outweighed the perceived privacy concerns otherwise they would not have decided in favor of their devices [e.g. 12, 13]. On the other hand, potential users might be deterred from using HWs due to perceived concerns. That is why another study should deal with HIPC and the influencing factors for potential users. Moreover, it would be interesting to analyze the effects of the GPDR implementation. Further research could evaluate, if stricter regulations influence individuals' privacy perception and whether new thematic maps with other factors occur.

References

[1] Angst, C.M., and Agarwal, R., "Adoption of Electronic Health Records in the Presence of Privacy Concerns: The Elaboration Likelihood Model and Individual Persuasion", Mis Quarterly, 33(2), 2009, pp. 339-370.

[2] Miltgen, C.L., Popovič, A., and Oliveira, T., "Determinants of End-user Acceptance of Biometrics: Integrating the 'Big 3' of Technology Acceptance with Privacy Context", Decision Support Systems, 56(1), 2013, pp. 103-114.

[3] Kenny, G., and Connolly, R., "Drivers of Health Information Privacy Concern: A Comparison Study ", Proceedings of the 22nd Americas Conference on Information Systems (AMCIS), 2016, pp. 1 - 10.

[4] Piwek, L., Ellis, D.A., Andrews, S., and Joinson, A., "The Rise of Consumer Health Wearables: Promises and Barriers", PLoS Med, 13(2), 2016, pp. e1001953.

[5] Agarwal, R., Gao, G., Desroches, C., and Jha, A.K., "Research Commentary—The Digital Transformation of Healthcare: Current Status and the Road Ahead", Information Systems Research, 21(4), 2010, pp. 796-809.

[6] Mc Afee, A., and Brynjolfsson, E., "Big data. The Management Revolution. ", Harvard Business Review, 90(10), 2012, pp. 61-67.

[7] Ermakova, T., Fabian, B., Kelkel, S., Wolff, T., and Zarnekow, R., "Antecedents of Health Information Privacy Concerns", Proceedings of the 5th International Conference on Current and Future Trends of Information and Communication Technologies in Healthcare (ICTH 2015), 2015, pp. 376-383.

[8] Plachkinova, M., Andrés, S., and Chatterjee, S., "A Taxonomy of mHealth Apps--Security and Privacy Concerns", Proceedings of the 48th Hawaii International Conference on Information System Sciences (HICSS), 2015, pp. 3187-3196.

[9] Alrige, M., and Chatterjee, S., "Toward a Taxonomy of Wearable Technologies in Healthcare", Proceedings of the 10th International Conference on Design Science Research in Information Systems and Technology (DESRIST), 2015, pp. 496-504.

[10] Braun, V., and Clarke, V.V., "Using Thematic Analysis in Psychology", Qualitative Research in Psychology, 3(2), 2006, pp. 77-101.

[11] Morton, A., "“All My Mates Have Got It, So It Must Be Okay”: Constructing a Richer Understanding of Privacy Concerns—An Exploratory Focus Group Study": Reloading Data Protection, Springer, 2014, pp. 259-298.

[12] Anderson, C.L., and Agarwal, R., "The Digitization of Healthcare: Boundary Risks, Emotion, and Consumer Willingness to Disclose Personal Health Information", Information Systems Research, 22(3), 2011, pp. 469-490.

[13] Li, H., Wu, J., Gao, Y., and Shi, Y., "Examining Individuals' Adoption of Healthcare Wearable Devices: An Empirical Study from Privacy Calculus Perspective", International Journal of Medical Informatics, 88(1), 2016, pp. 8-17.

[14] Culnan, M.J., and Bies, R.J., "Consumer Privacy: Balancing Economic and Justice Considerations", Journal of Social Issues, 59(2), 2003, pp. 323-342.

[15] Dinev, T., Xu, H., Smith, J.H., and Hart, P., "Information Privacy and Correlates: an Empirical Attempt to Bridge and Distinguish Privacy-related Concepts", European Journal of Information Systems, 22(3), 2013, pp. 295-316.

[16] Kotz, D., Gunter, C.A., Kumar, S., and Weiner, J.P., "Privacy and Security in Mobile Health: A Research Agenda", Computer, 49(6), 2016, pp. 22-30.

[17] Cohn, S.P., Privacy and Confidentiality in the Nationwide Health Information Network, National Committee on Vital and Health Statistics, Washington, USA, 2006.

[18] Hong, W., and Thong, J.Y.L., "Internet Privacy Concerns - An integrated Conceptualization and Four Empirical Studies", Mis Quarterly, 37(1), 2013, pp. 275-298.

[19] Smith, H.J., Milberg, S.J., and Burke, S.J., "Information Privacy: Measuring Individuals' Concerns About Organizational Practices", Mis Quarterly, 20(2), 1996, pp. 167-196.

[20] Malhotra, N.K., Kim, S.S., and Agarwal, J., "Internet Users' Information Privacy Concerns (IUIPC):
The Construct, the Scale, and a Causal Model", Information Systems Research, 15(4), 2004, pp. 336 - 355.

[21] Angst, C.M., "Protect My Privacy or Support the Common-Good? Ethical Questions About Electronic Health Information Exchanges", Journal of Business Ethics, 90(2), 2009, pp. 169-178.

[22] Chatterjee, S., and Price, A., "Healthy Living with Persuasive Technologies: Framework, Issues, and Challenges", Journal of the American Medical Informatics Association, 16(2), 2009, pp. 171-178.

[23] Varshney, U., "Mobile Health: Four Emerging Themes of Research", Decision Support Systems, 66(1), 2014, pp. 20-35.

[24] Morgan, D.L., "Focus Groups", Annual Review of Sociology, 22(1), 1996, pp. 129-152.

[25] Kitzinger, J., "Qualitative Research. Introducing Focus Groups", British Medical Journal, 311(7000), 1995, pp. 299-302.

[26] Patton, M.Q., Qualitative Research and Evaluation Methods, Sage Publications, Thousand Oaks, CA, 2002.

[27] Kari, T., Koivunen, S., Frank, L., Makkonen, M., and Moilanen, P., "Critical Experiences During the Implementation of a Self-Tracking Technology", Proceedings of the 20th Pacific Asia Conference on Information Systems (PACIS), 2016, pp. 1-16.

[28] Newell, S., and Marabelli, M., "Strategic Opportunities (and Challenges) of Algorithmic Decision-making: A Call for Action on the Long-term Societal Effects of 'Datification'", The Journal of Strategic Information Systems, 24(1), 2015, pp. 3-14.

[29] Becker, M., Kolbeck, A., Matt, C., and Hess, T., "Understanding the Continuous Use of Fitness Trackers: A Thematic Analysis", Proceedings of the 21th Pacific Asia Conference on Information Systems (PACIS), 2017, pp. 1-12.

[30] Stewart, K.A., and Segars, A.H., "An Empirical Examination of the Concern For Information Privacy Instrument", Information Systems Research, 13(1), 2002, pp. 36-49.